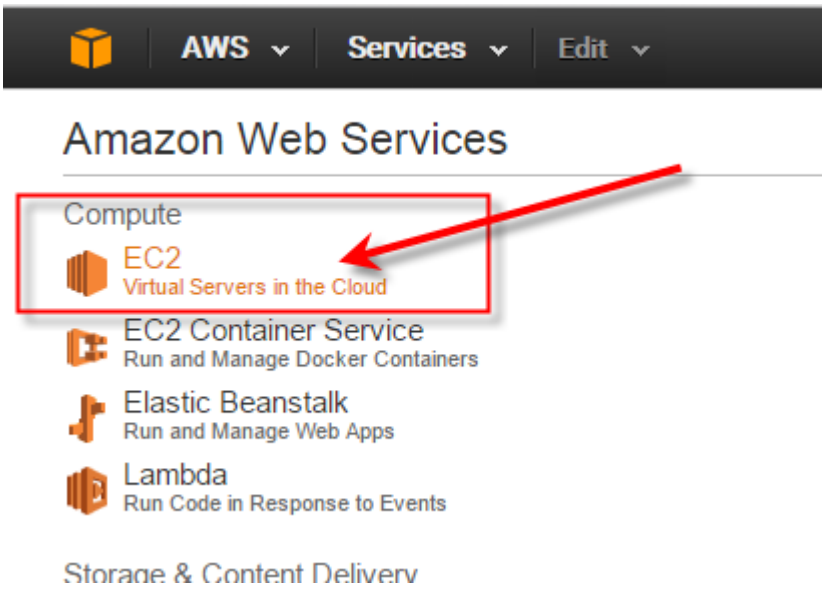
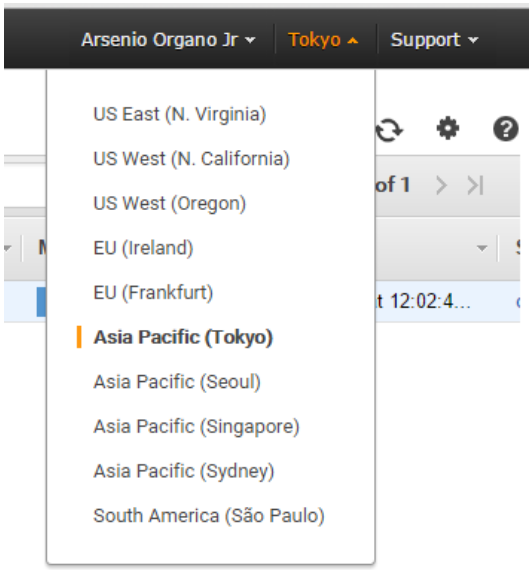
How to Setup Your Own Shadowsocks Using AWS EC2 to Bypass China's Internet Censorship



1. First, register a free account in Amazon Web Services and use their AWS Free Tier.

2. Once your registration has been approved, login now to your AWS console.

3. There are so many great services offered by Amazon but what you will only need is the **EC2** under **Compute**. Click that option.



4. Before launching your new instance, select the most suitable and closest country/region near where you are now. I opt to select Asia Pacific (Singapore) which I think is more stable and near China.

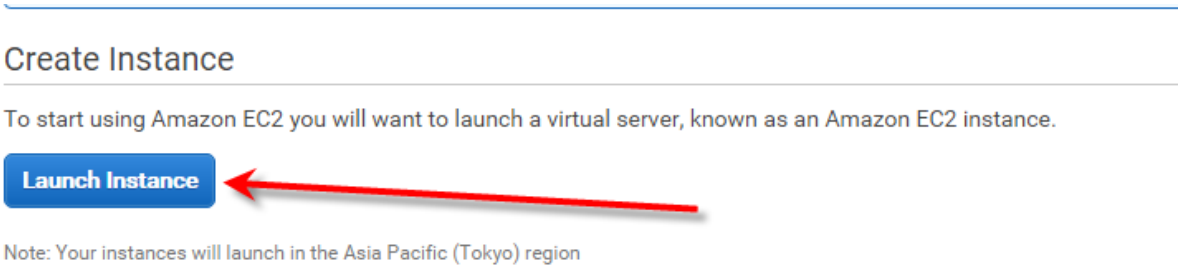
5. Then in your AWS EC2 Dashboard, you will need to create a new instance.

6. You will now go through a step-by-step installation. Don't

worry because it is not hard to follow. **TIP**: Just select the "Microsoft Windows Server 2012 R2 Base – ami-e3ba838d" free tier and press Next until you complete the whole setup.

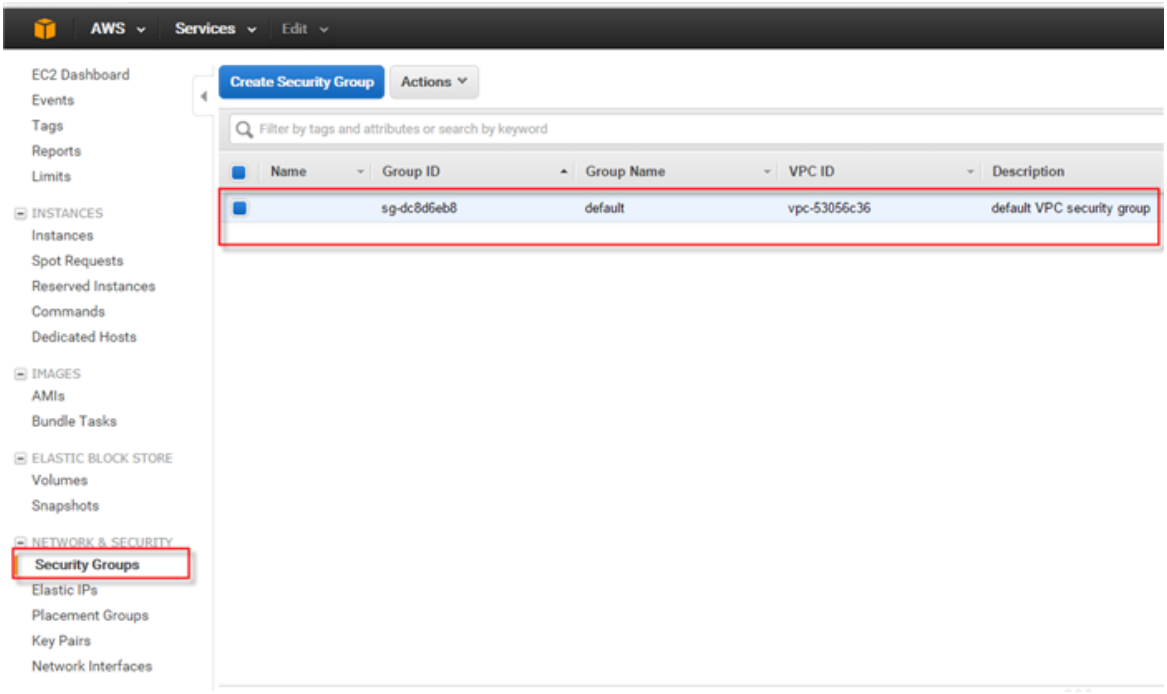
If you are Linux/UNIX savvy then you can go for it but for this tutorial I will only show the steps for Windows version. ALSO, stay with the FREE Tier or you might get charge like if you increase your disk space above 30GB.

By the way, during the installation you will be asked for the security group. You can choose the default (default VPC security group) or opt to create your own. The important thing is you take note of it because we will need to add rules for that later on.

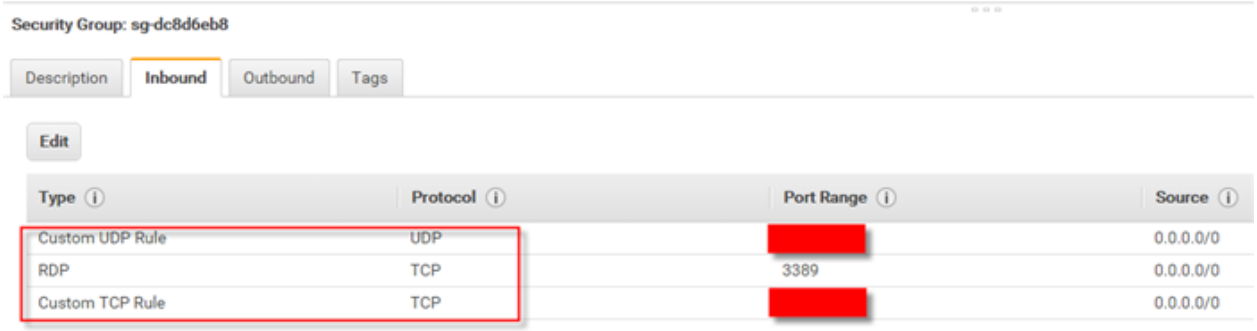


7. Once you have completed, you can launch the new instance you have created. Wait for approximately ~5 minutes before you proceed to the next step.

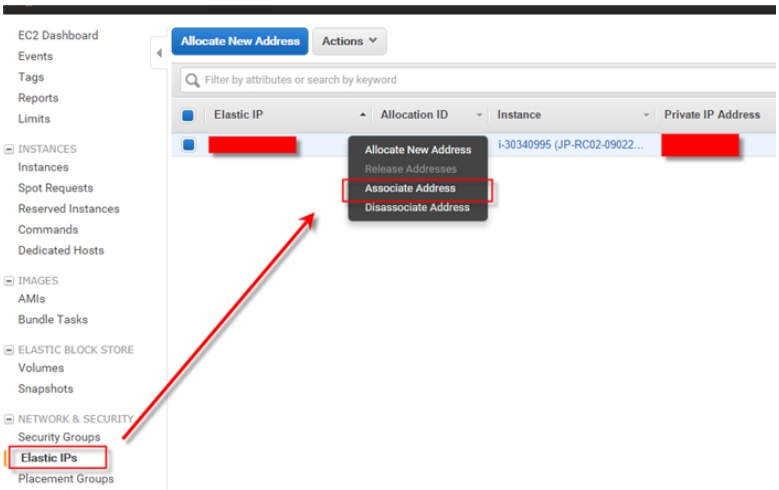
8. Let us setup your Security Group first. The key here is we need to add rules to the security group you either created or the default one which is associated with your instance. For example, my instance is associated with the default security group. Then that is the one we need to update. So expand the NETWORK & SECURITY and click **Security Groups**.



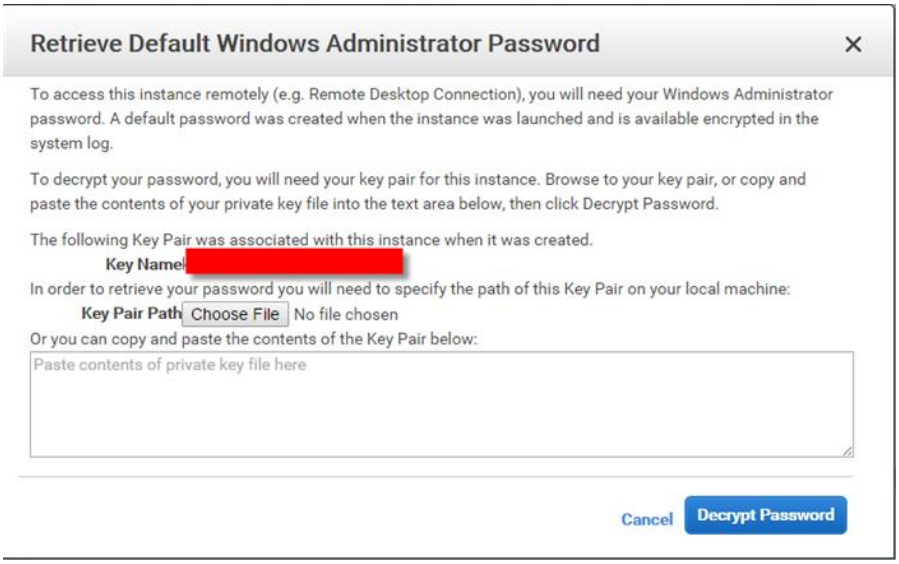
10. Then on the right-panel, under it click the **Inbound** tab.



11. Make sure you have RDP allowed in your Inbound because you will be using Remote Desktop tool to access your instance. Then the 2 next important tool is the "**Custom UDP Rule**" and "**Custom TCP Rule**" that you need to add. These 2 protocols will be valuable for setting up your Shadowsocks proxy. So all you have to do is add them with the port you want to use. ALWAYS use port 443! Make sure the ports for both are the same.



12. Then the next to configure, although optional, is the **Elastic IPs**. I recommend for you to set this up because you in case Amazon decides to refresh their system or a reboot needs to happen then you will need to go through accessing your AWS console again and checking the public IP address assigned to your instance. So from the same NETWORK & SECURITY Option, click **Elastic IPs** and associate your instance to the Public IP assigned to your instance.

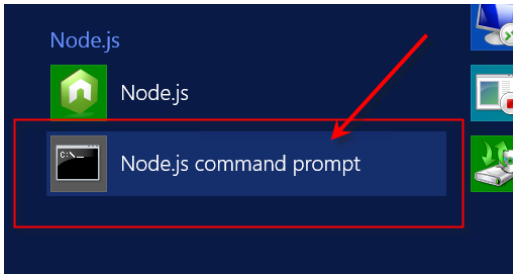


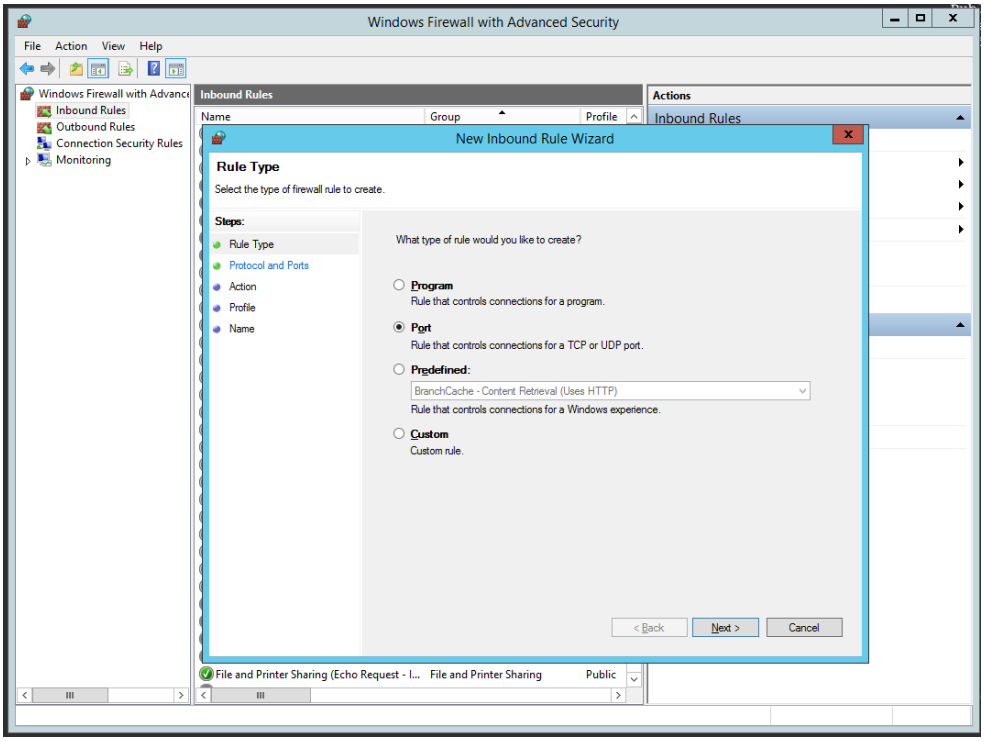
13. Then go to your AWS Console and click **Instances**. You will need a tool called Remote Desktop to access your new instance. But before you do that, you must get your Instance' password. So right-click your instance and click **Get Password**. This is a little bit tricky now but still easy. Remember during the installation process, you were given a password perm file (I hope you have not yet deleted it). You will need this option to decrypt so that you can obtain your password.

14. Once you have your password (keep it and also the perm file as you will need it in the future), open your Remote Desktop tool, put the public IP given to you and login as Administrator using the decrypted password.

15. You are now logged in to your instance. It's time to setup now your Shadowsocks VPN. Open your instance' browser, but I recommend you download and install either Google Chrome or Mozilla Firefox because the pre-installed Internet Explorer has a higher security and annoying pop-ups will keep on displaying while you are browsing. Go to https://nodejs.org/en/download/ and download the Windows Installer (.msi) for 64-bit.

16. Once it is installed, we need to configure the Node.JS. So click start and find the Node.js command prompt.





17. You must configure the Windows Firewall to allow incoming connections on port 443 (or whatever other port you set).

Open the Firewall and console and add a rule each for TCP and UDP on port 443 to allow connections from all addresses.

18. Then run this command below to continue with the installation. The installation will just take less than a minute – just few seconds.

```
npm install -g shadowsocks
```

19. Then open the Windows Explorer, and locate config.json file. It is found in:

```
C:\Users\Administrator\AppData\Roaming\npm\node_modules\shadowsocks
```

Open it with Notepad.

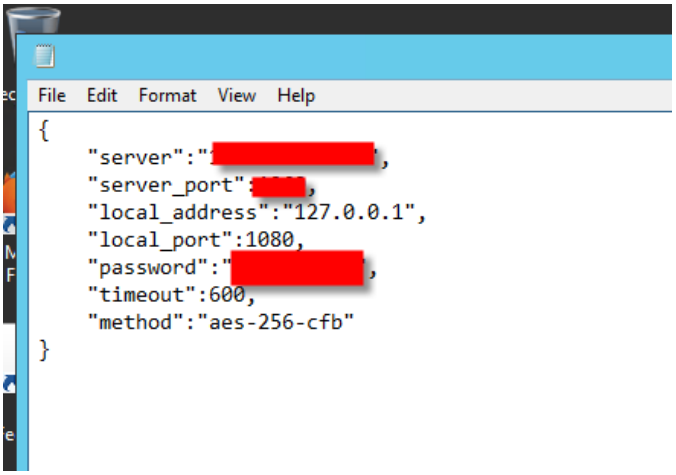
There are only 3 things that you need to change the values:

server: – put here the local IP address of your instance and NOT the public address

server_port: – put here the port number you add in the AWS Security group i.e. 443

password: – your own password

The others, leave them as they are good enough to use.

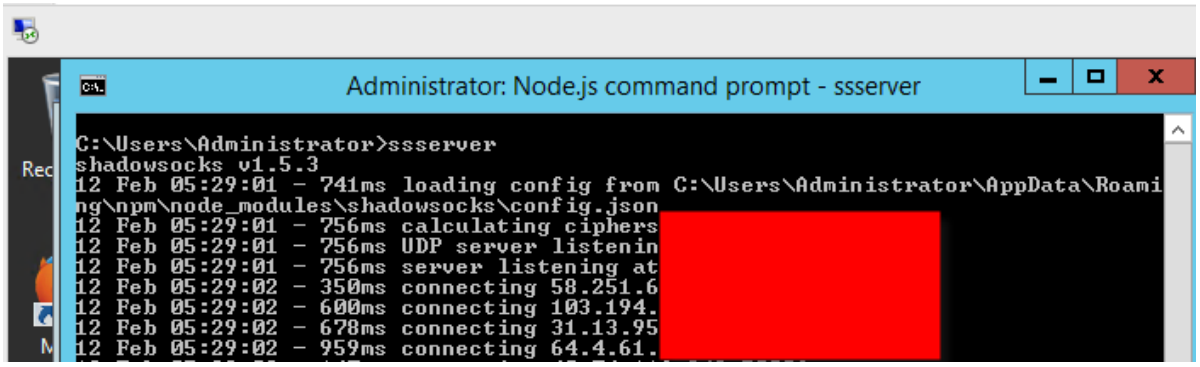


19. Save your changes and go back to your Node.js command prompt.

20. To start and invoke your proxy, just type:

```
ssserver
```

21. You will now see that the service has started



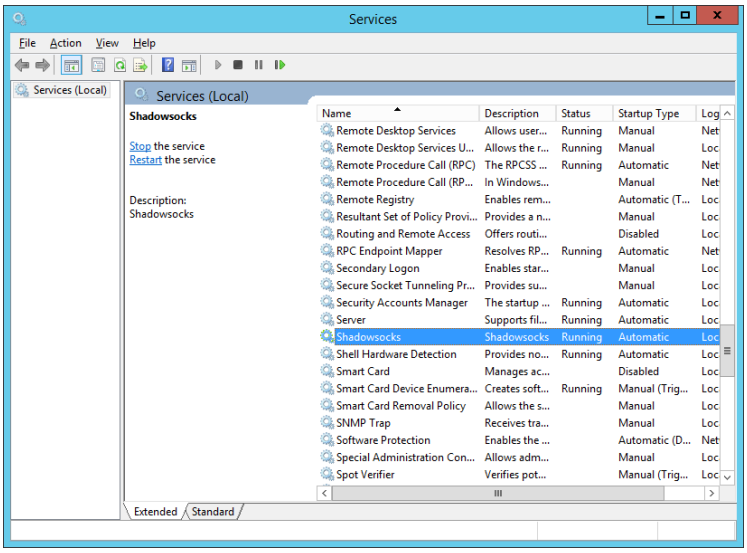
Connect a client and test the server. If the server works fine, you can proceed to the next step, otherwise find and resolve the problem.

22. You're nearly done – but not yet completely done. You have only setup the Shadowsocks proxy server but you need to set it so it operates as windows server, so it automatically restarts if windows is restarted. So here's how to do it:

Close the original Node.js command prompt running shadowsocks.

Start the Node.js command prompt again. Now type or copy/pasta

```
npm install -g node-windows

npm install -g qckwinsvc

qckwinsvc

prompt: Service name: Shadowsoscks

prompt: Service description: Shadowsoscks

prompt: Node script path:

C:\Users\Administrator\AppData\Roaming\npm\node_modules\shadowsocks\bin\ssserver

Service installed
```



Despite offering to start the service the service will NOT be started. Start the service manually using the services control panel.

Once the service shows as running, test the server as previously. Then re-boot the server in stance and test again after a few minutes that your shadowsocks server is running and operating correctly.

If so, you can pretty much forget about the server and just go surfing as I you are on the other side of the GFWOC. Monitor your usage and billing, any more than 30GB transfer per month is chargeable, so as much as you feel tempted to share this resource with friends, don't.